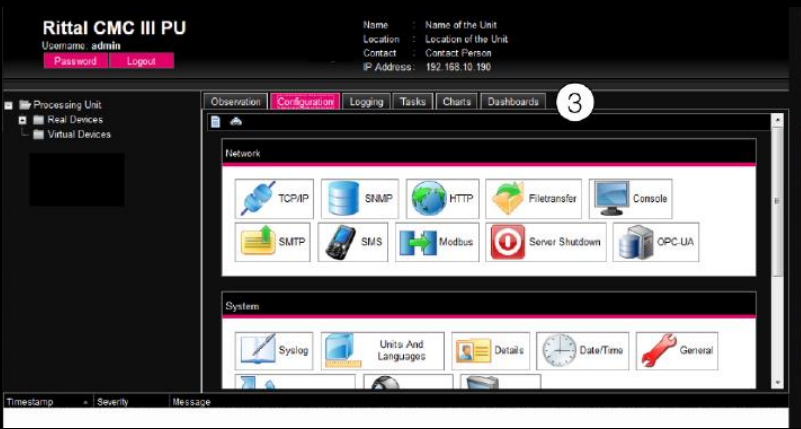


Rittal – The System.

Faster – better – everywhere.



Rittal Embedded Software Devices

System Hardening Guide

Inhaltsverzeichnis

1	Einleitung.....	3
2	Allgemeine Hinweise	3
3	Kommunikationskanäle.....	4
3.1	HTTP (Webzugriff)	4
3.2	Dateitransfer	5
3.3	Konsole.....	5
3.4	SMTP	6
3.5	SNMP	6
3.6	Modbus/TCP	6
3.7	OPC-UA.....	7
3.8	Digital I/O	7
4	Dateiaustausch und Updates	8
4.1	Aktuelle Sicherheits-Software.....	8
4.2	Aktuelle Firmware-Version	8
4.3	Schnittstellen.....	8
5	Zugangsberechtigungen	9
5.1	Admin Berechtigungen.....	10
5.2	Dateitransfer Berechtigung.....	10
5.3	Sichere Passwörter	10
5.4	Fernzugriffe	10
6	Reset auf Werkseinstellungen.....	11

1 Einleitung

Produkte, Netzwerke und Systeme müssen vor unberechtigten Zugriffen geschützt werden, um die Verfügbarkeit, die Vertraulichkeit und die Integrität von Daten zu gewährleisten.

Dies muss durch organisatorische und technische Maßnahmen umgesetzt werden. Für erhöhte Sicherheitsanforderungen empfiehlt Rittal die folgenden Maßnahmen zu beachten.

Dabei gibt es nicht nur Hinweise zur sicheren Nutzung, sondern auch zu konkreten Einstellungen am Gerät, die die Sicherheit erhöhen.

Es gilt in der Praxis immer abzuwägen, inwiefern eine der beschriebenen Änderungen angewandt werden sollte oder nicht.

Die verfügbaren Einstellungen können sich je nach eingesetztem Gerät unterscheiden.

Darüber hinaus finden Sie weiterführende Informationen auf den Webseiten des Bundesamts für Sicherheit in der Informationstechnik:

- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/allgemeine-empfehlungen_node.html

2 Allgemeine Hinweise

Bitte beachten Sie die allgemeinen IT-Sicherheitshinweise im Handbuch Ihres Gerätes.

- Betreiben Sie das Gerät nicht direkt im Internet, sondern nur in internen Netzwerken, die durch Firewalls nach außen abgesichert sind.
- Beschränken Sie die Zugangsberechtigungen zu den Geräten auf die Personen, die eine Berechtigung unbedingt benötigen.
- Beschränken Sie den physischen Zugang zu den Geräten durch geeignete Maßnahmen.
- Sämtliche Schnittstellen, beispielsweise die USB-Anschlüsse, dürfen nicht aus dem sicheren Schaltschrank herausgeführt oder dorthin verlängert werden.

3 Kommunikationskanäle

Grundsätzlich gilt das Sie alle nicht genutzten Kommunikationskanäle am Gerät deaktivieren sollten.

Darüber hinaus stehen für viele Protokolle Alternativen mit höherer Sicherheit zu Verfügung. Hier wird empfohlen die unsichere Variante zu deaktivieren. Bei einigen Protokollen kann die Sicherheit noch durch weitere Einstellungen erhöht werden.

Um geeignete Härtingsmaßnahmen für das Gerät zu ermitteln, kann es hilfreich sein, sich einen Überblick über alle verfügbaren Managementprotokolle und Schnittstellen zu verschaffen, die als Angriffsziele dienen könnten.

Schnittstelle	Internetzugang vorgesehen	Verschlüsselung unterstützt
HTTP	NO	NO
HTTPS	NO	YES
SNMP	NO	YES
Modbus TCP	NO	NO
OPC UA	NO	YES
RS232 / RS485	NO	NO
Rittal Sensor Bus (CAN)	NO	NO
USB (Massenspeicher & seriell)	NO	NO
Digital I/O	NO	NO
Physische Tasten	NO	NO

Tabelle 1

3.1 HTTP (Webzugriff)

Der Zugriff auf die Webseite des Gerätes darf nur über HTTPS erfolgen. Dabei wird empfohlen das "Security Level" auf "Modern" zu setzen um die Nutzung von TLS 1.3 zu forcieren.

HTTP-Einstellungen

Standard Zugriff (ohne SSL)

Port

80

Aktivieren ☐

Sicherer Zugriff (mit SSL)

SSL-Port

443

SSL Aktivieren ☒

Sicherheitslevel Modern

Warnung: HTTP ist eingeschaltet. Aus Sicherheitsgründen sollte nur HTTPS verwendet werden.

Speichern

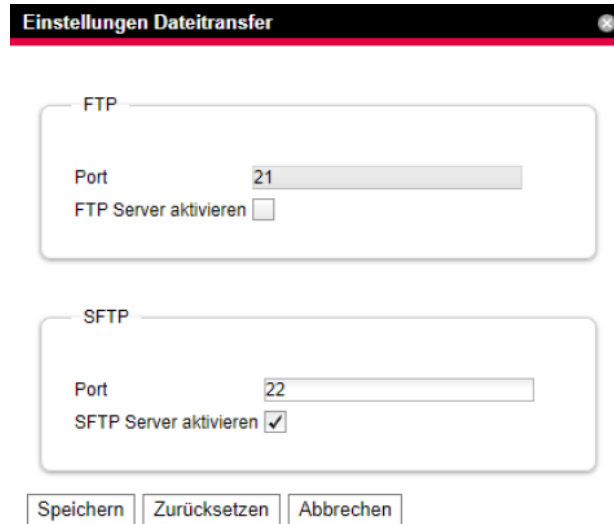
Zurücksetzen

Abbrechen

Abbildung 1: HTTP Einstellungen

3.2 Dateitransfer

Der Zugriff auf das Gerät über FTP/SFTP ist generell zu deaktivieren. Der SFTP Zugang sollte nur für die Dauer einer Aufgabe (z.B. Software-Update oder Datensicherung, siehe Handbuch) aktiviert werden.



Einstellungen Dateitransfer

FTP

Port 21

FTP Server aktivieren ☐

SFTP

Port 22

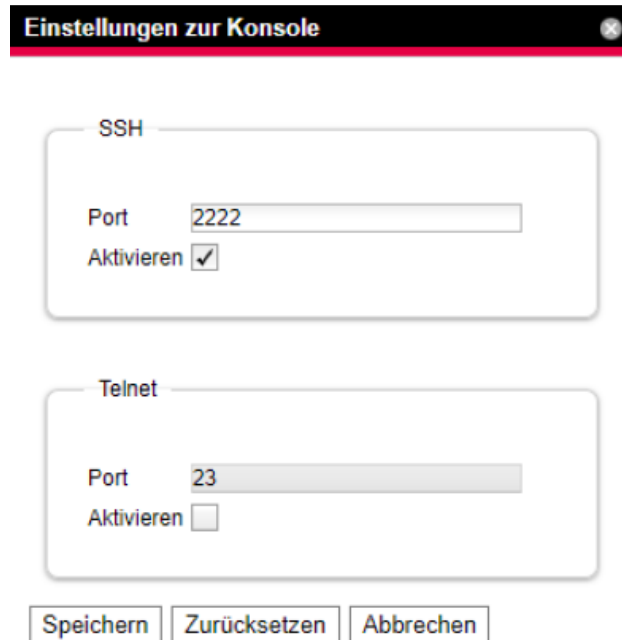
SFTP Server aktivieren ☒

Speichern Zurücksetzen Abbrechen

Abbildung 2: Einstellungen Dateitransfer

3.3 Konsole

Es wird empfohlen den Konsolen Zugang über Telnet komplett zu deaktivieren, da die Übertragung unverschlüsselt erfolgt.



Einstellungen zur Konsole

SSH

Port 2222

Aktivieren ☒

Telnet

Port 23

Aktivieren ☐

Speichern Zurücksetzen Abbrechen

Abbildung 3: Einstellungen zur Konsole

3.4 SMTP

Bei der Nutzung von SMTP ist zu beachten, dass der genutzte Mailserver Authentifizierung und Verschlüsselung unterstützt.

Abbildung 4: SMTP Einstellungen

3.5 SNMP

Bei der Verwendung von SNMP ist darauf zu achten, nur Version 3 einzusetzen, da Version 1 und 2 keine Möglichkeiten der Authentifizierung und Verschlüsselung bieten.

In den Einstellungen wird empfohlen die "Authentifizierungsmethode auf "SHA" und die "Privatsphäre" auf "AES" zu stellen. Außerdem sind die Standard Communities „public“ bei SNMP zu überschreiben.

Aktuell wird auf dem Gerät bei SNMP nur SHA1 unterstützt, sollte dies in der Anwendung/Umgebung nicht den Anforderungen entsprechen, darf SNMP nicht genutzt werden.

Bei der Passwortvergabe ist zu beachten, dass dieses den im Kapitel "Sichere Passwörter" vorgestellten Regeln genügt.

Weiterhin wird empfohlen in der Sektion "Allowed Hosts" alle Hosts einzutragen, welche über SNMP auf das Gerät zugreifen dürfen.

Abbildung 5: SNMP Einstellungen

3.6 Modbus/TCP

Das Modbus Protokoll bietet keine Authentifizierungs- und Verschlüsselungs-Funktion und von der Nutzung wird daher abgeraten.

Lässt sich der Einsatz nicht vermeiden, wird empfohlen, die Hosts, welche über Modbus auf das Gerät zugreifen dürfen, in der Sektion "Allowed Hosts"

einzutragen. Außerdem wird empfohlen, den Zugriff wenn möglich auf "lesenden Zugriff" zu beschränken.

No.	Host	Access Rights
1	155.155.155.155	read
2		read
3		read
4		read
5		read
6		read

Abbildung 6: Modbus Konfiguration

3.7 OPC-UA

Aktuell bieten die Geräte keine Möglichkeit Zugriffe über OPC-UA zu verschlüsseln. Wenn OPC-UA dennoch benötigt wird, wir empfohlen, die Benutzer Authentifizierung unter dem Dropdown "Security" anschalten und ein sicheres Passwort zu vergeben.

Abbildung 7: OPC-UA Konfiguration

3.8 Digital I/O

Das Gerät bietet die Möglichkeit, digitale Ein- und Ausgänge über Master-Protokolle und Aufgaben zu überwachen und zu steuern. Im Gegenzug können Aufgaben von dazu berechtigten Benutzern so konfiguriert werden, dass sie Systemzustände und Ausgaben an übergeordnete Systeme beeinflussen. Zudem können kritische Systemzustände abgerufen werden, wenn eine Aufgabe so konfiguriert ist, dass sie das Alarmrelais entsprechend schaltet.

Name	Value
☒ PDU-Controller	
☒ Device	OK
☒ Input (Input)	Off
DescName	Input
Value	0
Logic	0: Off / 1: On
Delay	1,0 s
Status	Off
☒ Alarm Relay (Output)	Off
DescName	Alarm Relay
Relay	Off
Logic	0: Off / 1: On
Status	Off
☒ System	

Abbildung 8: Konfiguration von digitalen Ein- und Ausgängen

Daher ist bei der Platzierung von Signalquellen und -senken für digitale Ein-/Ausgänge besondere Sorgfalt geboten. Darüber hinaus sind Aufgaben und Automatisierungen auf Mastersystemen sorgfältig zu konfigurieren.

Monitoring		Configuration	Logging	Tasks	Charts	Dashboards	Access Configuration
ID	Name	Description			Enabled		
1	Button monitoring	Switch off server if button has been pressed			Yes		
2	Task 2				No		
3	Task 3				No		

Abbildung 9: Task Konfiguration auf einem Rittal Gerät

4 Dateiaustausch und Updates

4.1 Aktuelle Sicherheits-Software

Für die Identifizierung und Eliminierung von Sicherheitsrisiken wie Viren, Trojanern und anderer Schadsoftware, wird empfohlen auf allen PCs eine Sicherheits-Software installiert zu haben und diese aktuell zu halten.

Jegliche Daten, die auf das Gerät gespielt werden, sind vom Anwender zu überprüfen.

4.2 Aktuelle Firmware-Version

Stellen Sie sicher, dass auf allen Geräten die aktuelle Rittal – Firmware verwendet wird. Die Firmware wird auf den jeweiligen Produktseiten im Internet zum Download bereitgestellt.

4.3 Schnittstellen

Obwohl das Gerät nur bekannte und signierte Daten vom Gerät akzeptiert und verarbeitet, wird empfohlen, die Schnittstellen (z.B. USB) zu deaktivieren.

Dies erfolgt im Bereich Überwachung und die Einstellung findet sich dann im Gerätebaum unter dem Punkt "Memory". Dort kann das entsprechende "Command" zum Abschalten der USB-Schnittstelle ("Aus") geschrieben werden.

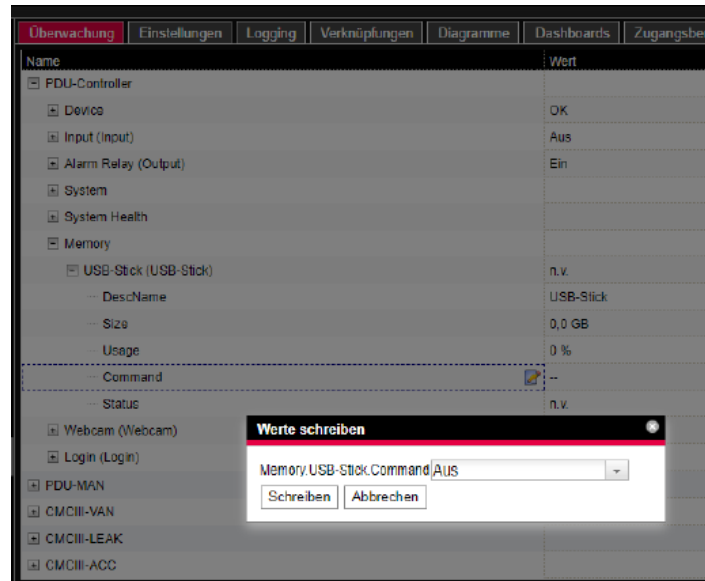


Abbildung 10: USB-Stick Konfiguration

5 Zugangsberechtigungen

Nicht genutzte Benutzerkonten sind zu deaktivieren.

Sofern möglich, wird der Einsatz von zentralen Nutzerverwaltungen für das User-Management und die Anmeldeinformationen empfohlen. Rittal-Produkte unterstützen LDAP und RADIUS.

Die lokale Benutzerdatenbank auf jedem Gerät ist in Benutzergruppen unterteilt. Für Gruppen und Benutzer lassen sich Berechtigungen festlegen, die sich auf die Web-Oberfläche sowie den allgemeinen Zugriff auf die Protokolle des Gerätes auswirken.

In der Benutzerkonfiguration können berechtigte Nutzer Konten aktivieren, Berechtigungen für Dateiübertragungsprotokolle (FTP & SFTP) sowie für den Zugriff auf die Web-Oberfläche (HTTP/HTTPS) erteilen und die Zugriffsrechte für die Nutzung der seriellen Konsole (SSH, Telnet & USB) verwalten.

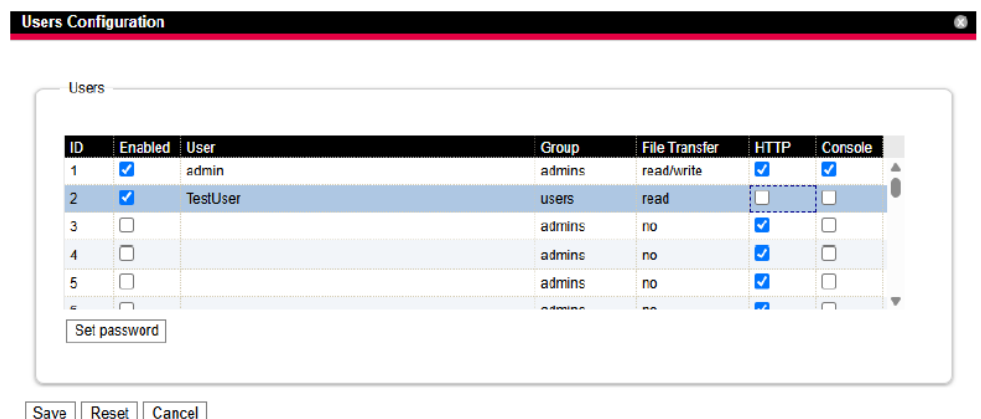


Abbildung 11: Benutzer Konfiguration

Benutzer werden Benutzergruppen zugewiesen. In der Gruppenkonfiguration der Web-Oberfläche lassen sich das Timeout sowie die Berechtigungen für Sensoren gemäß dem Produkthandbuch verwalten.

5 Zugangsberechtigungen

DE

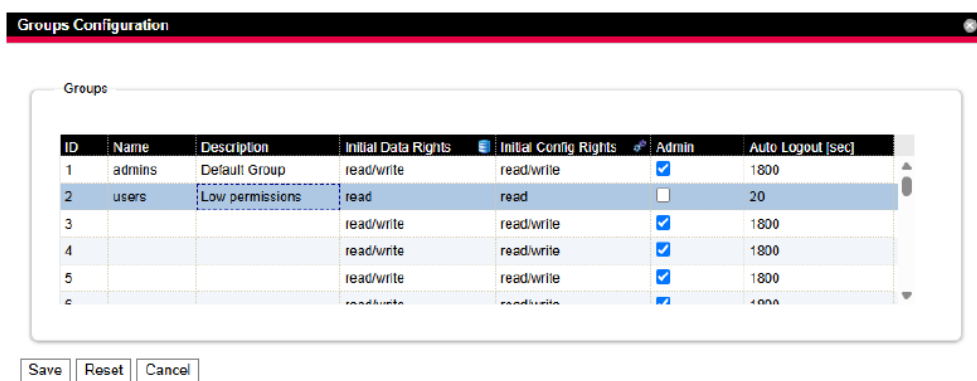


Abbildung 12: Gruppenkonfiguration

Wie auf den Screenshots zu sehen ist, kann ein berechtigter Benutzer sowohl Administratorenkonten mit umfassenden Rechten wie auch Konten mit eingeschränktem Zugriff auf das Gerät erstellen.

5.1 Admin Berechtigungen

Beachten Sie, dass Nutzer, welche einer Gruppe mit aktiviertem Admin-Flag angehören, über das Web Management Interface Zugriff auf die komplette Gerätekonfiguration haben und alle Einstellungen herunterladen und bearbeiten können.

Die Zahl der Benutzer mit Admin Berechtigungen bzw. Admin Gruppen Zugehörigkeit ist auf notwendige vertrauenswürdige Personen zu beschränken.

5.2 Dateitransfer Berechtigung

Nutzer bei denen der Dateitransfer erlaubt ist, können auf alle auf dem Gerät liegenden Daten zugreifen und bei aktiviertem Schreibzugriff auch verändern. Dazu gehören auch Statusinformationen und Gerätekonfiguration. Dies erfolgt unabhängig der Zugehörigkeit zu einer Gruppe mit aktiviertem Admin Flag.

Der Dateitransfer ist daher nur für Benutzer zu aktivieren, welche Mitglied in einer Gruppe mit Admin Flag sind und es sollte, wenn möglich, auf schreibenden Zugriff verzichtet werden. Nutzer mit Dateitransfer Berechtigung sind als Administratoren anzusehen.

5.3 Sichere Passwörter

Verwenden Sie keine Standard-Passwörter, sondern sichere, lange Passwörter, die Zahlen, große/ kleine Buchstaben, Zeichen und keine Wiederholungen beinhalten. Erzeugen Sie nach Möglichkeit zufällige Passwörter mit einem Passwort-Manager.

Passwörter sollten nach einem gewissen Zeitraum aktualisiert werden. Rittal-Produkte geben keine Rückmeldung darüber, wie alt ein Passwort ist. Die Verantwortung hierfür liegt beim Überwachungssystem oder bei einem externen Kontenanbieter, wie etwa einem LDAP- oder RADIUS-Server.

5.4 Fernzugriffe

Bei der Nutzung von Fernzugriffen ist ein sicherer Zugriffsweg wie VPN (Virtual Private Network) oder HTTPS zu wählen.

6 Reset auf Werkseinstellungen

Um das Gerät zurückzusetzen und alle Daten und Einstellungen zu löschen sind folgende Schritte erforderlich:

- Gerät vom Strom trennen.
- Die Display Taste unter dem R des Rittal-Aufdrucks gedrückt halten
- Gerät mit Spannung versorgen und Taste gedrückt halten bis die Status LED Rot reagiert.
- Ausführen der Wiederherstellung ist erkennbar am weißen Blitz der Status LED.

Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

You can find the contact details of all
Rittal companies throughout the world here.



www.rittal.com/contact

RITTAL GmbH & Co. KG
Postfach 1662 · 35726 Herborn · Germany
Phone +49 2772 505-0 · Fax +49 2772 505-2319
E-mail: info@rittal.de · www.rittal.com

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

